ANDROID STATIC ANALYSIS REPORT

app_icon

GPSMapAppDiego (1.0)

File Name:	app-debug.apk
Package Name:	com.example.gpsmapappdiego
Scan Date:	Oct. 28, 2024, 3:33 a.m.
App Security Score:	44/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	2	0	1	1

FILE INFORMATION

File Name: app-debug.apk
Size: 12.79MB
MD5: 786dd21d2ce0127092e53c531f217555
SHA1: 9d3b2ee559909d026bbd72ed673629b99f000fed
SHA256: c4dde1b4a640ee9ec08e8bf1083d964f2004ce647ec7bd8a6e291e131516b7cb

APP INFORMATION

App Name: GPSMapAppDiego
Package Name: com.example.gpsmapappdiego
Main Activity: com.example.gpsmapappdiego.MainActivity
Target SDK: 34
Min SDK: 30
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 2
Services: 0
Receivers: 1
Providers: 1
Exported Activities: 0
Exported Services: 0
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: CN=Android Debug, O=Android, C=US
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-09-12 16:25:31+00:00
Valid To: 2054-09-05 16:25:31+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha256
md5: d1e354905a8af489f7e601a238af02fc
sha1: 7b20a0a1dbc1945041cabd3ac8243330e13bca11
sha256: a2fa84d98cba79cc44aefe4a4237e05cab2b7d33d452cb2e858ed13be4e536a6
sha512: 37aee483cb9e6fe4da748ce5dbf2ad79419342721f70dda3e718298deb35076c4809cbf3031a230b903c982aff028bbfb55035b35d8eee2df58c83ca636526f9
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: c136c47318927e7d2f3626d4779ad6a8e3d50a7c4ba565bbae5a237d79fd91ea
Found 1 unique certificates
```

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.example.gpsmapappdiego.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes4.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table></td></tr>
<tr><td>classes3.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table></td></tr>
<tr><td>classes2.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.BRAND check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **1** | WARNING: **0** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

TITLE	SEVERITY	DESCRIPTION
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **2** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	4/24	android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET
Other Common Permissions	0/45	

Malware Permissions:

Top permissions that are widely abused by known malware.

Other Common Permissions:

Permissions that are commonly abused by known malware.

HARDCODED SECRETS

POSSIBLE SECRETS
"google_maps_key" : "AIzaSyDwCnXzg8SvVQk_YzXt7Ri4iWSGHjYUQwc"

SCAN LOGS

Timestamp	Event	Error
2024-10-28 03:33:28	Generating Hashes	OK
2024-10-28 03:33:28	Extracting APK	OK
2024-10-28 03:33:28	Unzipping	OK
2024-10-28 03:33:28	Getting Hardcoded Certificates/Keystores	OK
2024-10-28 03:33:29	Parsing AndroidManifest.xml	OK
2024-10-28 03:33:29	Parsing APK with androguard	OK
2024-10-28 03:33:30	Extracting Manifest Data	OK
2024-10-28 03:33:30	Performing Static Analysis on: GPSMapAppDiego (com.example.gpsmapappdiego)	OK
2024-10-28 03:33:30	Fetching Details from Play Store: com.example.gpsmapappdiego	OK

2024-10-28 03:33:31	Manifest Analysis Started	OK
2024-10-28 03:33:31	Checking for Malware Permissions	OK
2024-10-28 03:33:31	Fetching icon path	OK
2024-10-28 03:33:31	Library Binary Analysis Started	OK
2024-10-28 03:33:31	Reading Code Signing Certificate	OK
2024-10-28 03:33:31	Running APKiD 2.1.5	OK
2024-10-28 03:33:35	Updating Trackers Database....	OK
2024-10-28 03:33:35	Detecting Trackers	OK
2024-10-28 03:33:36	Decompiling APK to Java with jadx	OK
2024-10-28 03:33:45	Converting DEX to Smali	OK
2024-10-28 03:33:45	Code Analysis Started on - java_source	OK

2024-10-28 03:35:01	Android SAST Completed	OK
2024-10-28 03:35:01	Android API Analysis Started	OK
2024-10-28 03:36:22	Android Permission Mapping Started	OK
2024-10-28 03:36:29	Android Permission Mapping Completed	OK
2024-10-28 03:36:29	Finished Code Analysis, Email and URL Extraction	OK
2024-10-28 03:36:29	Extracting String data from APK	OK
2024-10-28 03:36:29	Extracting String data from Code	OK
2024-10-28 03:36:29	Extracting String values and entropies from Code	OK
2024-10-28 03:36:30	Performing Malware check on extracted domains	OK
2024-10-28 03:36:30	Saving to Database	OK

Report Generated by - MobSF v4.0.7

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.